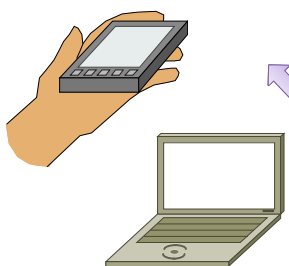
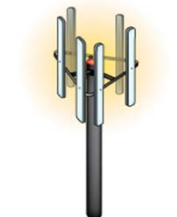
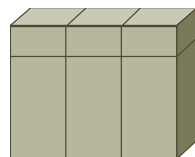
資料１－３

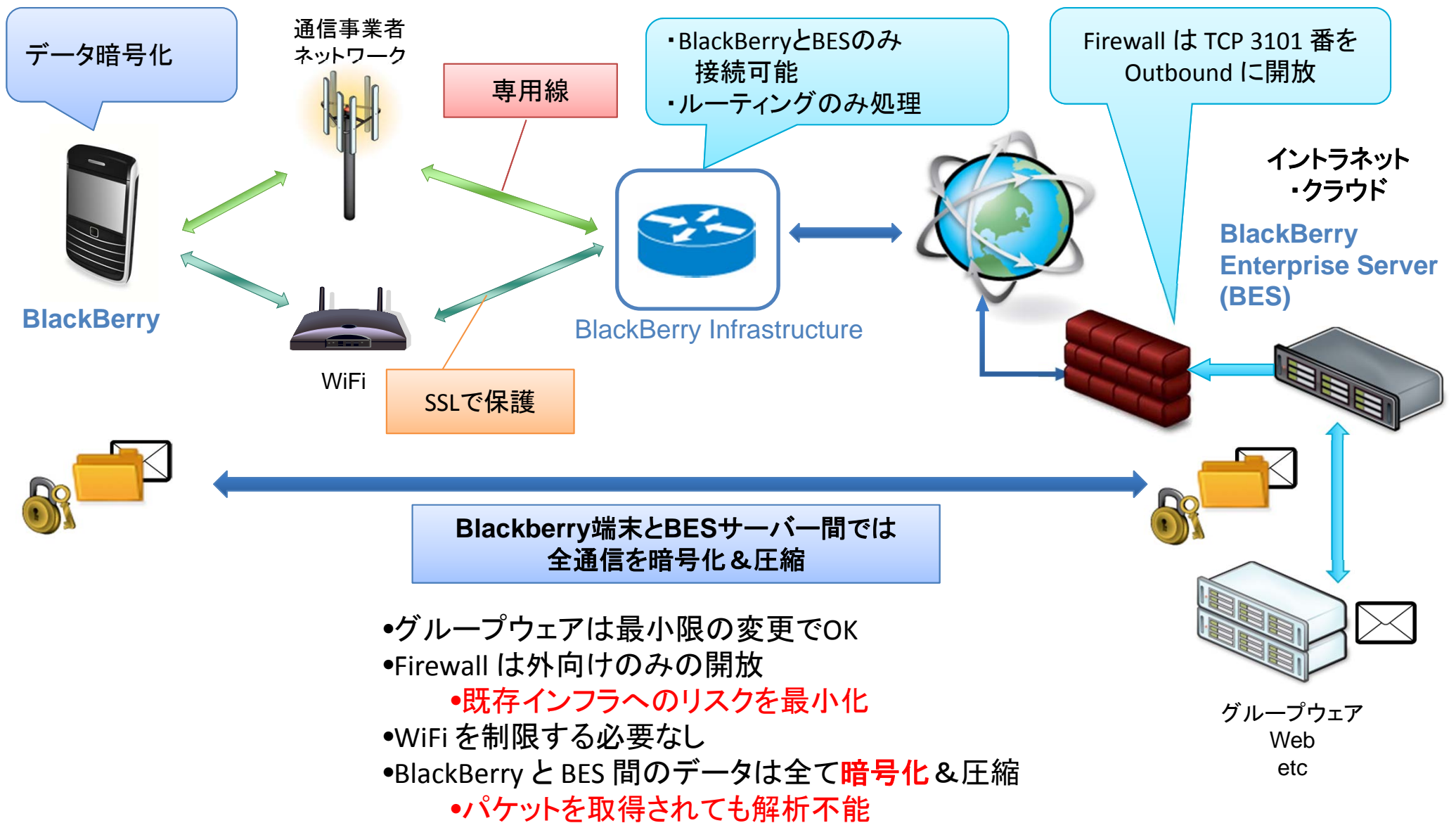
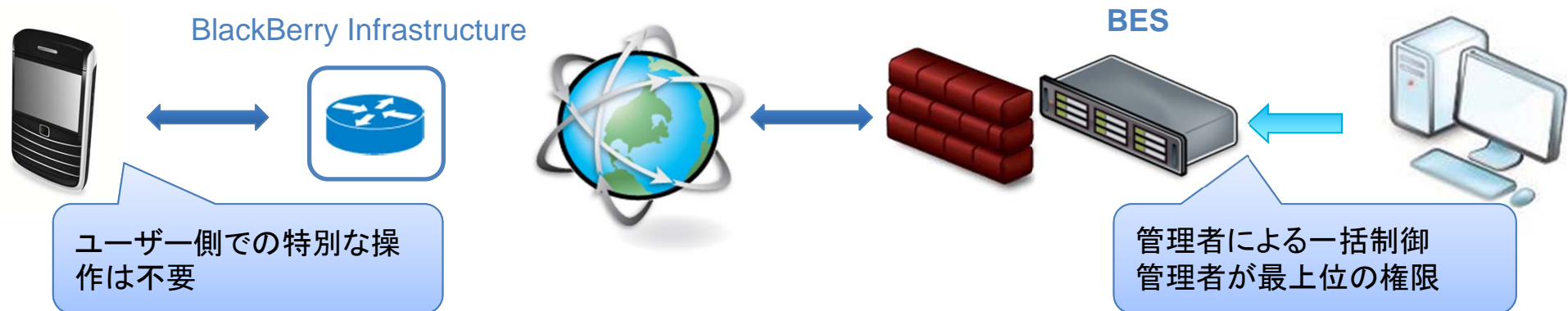
スマートフォンにおけるセキュリティについて

2011年2月24日
株式会社NTTドコモ

BlackBerryのセキュリティについて

他社スマートフォン
PC
端末側にて全ての機能を処理
通信事業者
ネットワーク
メール
Web
etc
WiFi
BlackBerry
BlackBerry Infrastructure
BlackBerry Infrastructure を経由
端末とサービスで処理を分担

docomo

- グループウェアは最小限の変更でOK
- Firewall は外向けのみの開放
    - 既存インフラへのリスクを最小化
- WiFi を制限する必要なし
- BlackBerry と BES 間のデータは全て**暗号化**＆圧縮
    - パケットを取得されても解析不能

セキュリティの集中管理

docomo

- BES管理者によるセキュリティ設定（ITポリシー）
  - 450以上の設定項目にて、企業のポリシーを適用
  - 大量の端末を簡単・効率的に管理
  - 端末の設定、アプリ、各種サービスの利用可否
    - 管理者が許可しないアプリはインストール不可
  - 全てワイヤレスで集中管理
- 利用状況、資産管理
  - 利用状況、端末の状態等を定期的にBES側で取得

ITポリシーによる制御例

- パスワード(有効期間、パターン、最小文字数、履歴・・・)
- SMS禁止、電話禁止、ブラウザ禁止、モデムとしての利用禁止
- 添付ファイルのサイズ制限
- サードパーティアプリの自動配布・使用制限
- SDカード禁止、Bluetooth禁止、マスストレージの禁止
- コピー＆ペーストの禁止、画面ショットの取得禁止
- 端末内部データの暗号化の強制
- BISの利用を制限
- BESを経由しない通信は全て禁止
- 自動ワイプアウト(データ初期化)
  - XX時間ロックが解除されなかったら・・・、YY時間BESとの
  - 通信が無い・・・、バッテリーが極端に消耗したら・・・、
  - ZZ回パスワードを間違えたら・・・

個人でBISを利用している端末も、BESの制御下に！

端末が圏外の状況下でもデータを保護！

- **機密性を保障する暗号化**
  - BlackBerryから送受信される全てのデータはAES もしくは 3DESにて保護
  - BlackBerry上に保存される全てのデータはAESにて保護
  - モジュールの自己テストと整合性チェック

- **堅牢なリモートIT管理**
  - ワイヤレス管理と構成制御
  - 450 以上のポリシー制御を、サーバーから制御
  - リモートでの端末のロック、ワイプ、自動ワイプ

- **複数のユーザー認証方法**
  - パスワード管理と制御

- **長さ、複雑さ, 有効期限, セッションタイムアウト, 履歴**
  - スマートカード、RSAによる二要素認証機能
    - http://www.blackberry.com/go/smartcardreader

- セキュアブートロムと署名API
  - BlackBerryはOSを保護
  - 許可されたアプリケーションのみが稼動
  - APIおよびユーザーデータアクセスに関する詳細なIT制御

- 独立したセキュリティ監査と検証 – “信頼と実証”
  - 各国の認可
  - 情報技術セキュリティ評価基準
  - Fraunhofer Institute Certification …

脆弱性のないコミュニケーションを: BlackBerry のセキュリティ認可

docomo

各国政府の認可

NATO
NATO RESTRICTED

United Kingdom
RESTRICTED

Netherlands
Not specified

Canada
Protected B

Australia
RESTRICTED

Turkey
Not specified

United States
SBU

New Zealand
RESTRICTED

Austria
Not specified

情報技術セキュリティ評価基準 (Common Criteria)

認証機関

•ワイヤレスプラットフォームで初、かつ唯一のCommon Criteria EAL 4+ 認定を獲得！

モバイル化のリスクを最小化し、企業データを保護

1. 端末
   – 堅牢なハード・ソフトウェア & データの保護
   – サーバーからの一括管理(ITポリシー)
2. 企業ネットワーク
   – セキュリティ強度を維持して導入が可能
3. 通信
   – 端末とサーバーの間の通信の暗号化

スマートフォンにおけるセキュリティについて

- spモード

  - アクセス制限サービス

    有害ウェブサイトなどからお子さまを守る、ドコモのフィルタリングサービスです。アクセス制限されるサイトやカテゴリの一部などを設定することにより、変更することができます。
  - メールウイルスチェック

    メールを通して感染するウイルスから、スマートフォンを保護するサービスです。メールの送受信時にドコモでチェックを行い、ウイルスを検知した場合は即座に駆除(削除)します。
- ドコモマーケット
  - スマートフォン向けポータルサイトです。おすすめのコンテンツやアプリケーションをドコモが分かりやすく紹介することで、お客様が必要なものをより簡単にお探しいただけます。
  - ドコモマーケットへのアプリ掲載は、ドコモで審査しています。
- スマートフォン遠隔制御サービス
  - 企業で利用・管理しているスマートフォン端末に、インストールしたアプリケーションを制御する事で、スマートフォン端末を安心、便利にご利用いただくためのASPサービスです。
  - 端末紛失時のロックやデータ削除、発信先制限、デバイス利用制限等、管理画面上より一括して実施可能
- 取扱説明書へ記載
  - 次ページ資料参照

取扱説明書(注意事項)へ記載

- 本FOMA端末はパソコンなどと同様に、お客様がインストールを行うアプリケーションなどによっては、お客様のFOMA端末の動作が不安定になったり、お客様の位置情報やFOMA端末に登録された個人情報などがインターネットを経由して外部に発信され、不正に利用されたりする可能性があります。このため、ご利用になるアプリケーションなどの提供元および動作状況について十分にご確認の上、ご利用ください。

目次／注意事項

- 本FOMA端末はパソコンなどと同様に、お客様がインストールを行うアプリケーションなどによっては、お客様のFOMA端末の動作が不安定になったり、お客様の位置情報やFOMA端末に登録された個人情報などがインターネットを経由して外部に発信され、不正に利用されたりする可能性があります。このため、ご利用になるアプリケーションなどの提供元および動作状況について十分にご確認の上、ご利用ください。

SC-01Cをご利用にあたっての注意事項

- 本FOMA端末は、iモードのサイト（番組）への接続やiアプリなどには対応しておりません。
- 本FOMA端末は、データの同期や最新のソフトウェアバージョンをチェックするための通信、サーバとの接続を維持するための通信など一部自動的に通信を行う仕様となっています。また、動画の視聴などを行うと、大量のパケット通信が発生します。このため、「パケ・ホーダイ ダブル／パケ・ホーダイ シンプル」などのパケット定額サービスのご利用を強くおすすめします（なお、「パケ・ホーダイ ダブル／パケ・ホーダイ シンプル」ご契約の場合、短期間で上限額に達します）。
- 公共モード（ドライブモード）には対応しておりません。
- 本FOMA端末は、オペレーティングシステム（OS）のバージョンアップにより機能が追加されたり、操作方法が変更になったりすることがあります。機能の追加や操作方法の変更などに関する最新情報は、ドコモのホームページでご確認ください。
- OSをバージョンアップすると、古いバージョンのOSで使用していたアプリケーションが使えなくなる場合や意図しない不具合が発生する場合があります。
- 万が一紛失した場合は、Googleトーク、Gmail、AndroidマーケットなどのGoogleサービスやFacebook、Twitter、mixiを他の人に利用されないように、パソコンより各種サービスアカウントのパスワードを変更してください。
- spモード、mopera UおよびビジネスmoperaインターネットI以外のプロバイダはサポートしておりません。